

# 

Statement of Work

Security Modernization

Prepared for

Prepared by

Date: March 18, 2020

Version: 1.0

Table of contents

[Introduction 1](#_Toc35424789)

[1. Project objectives and scope 1](#_Toc35424790)

[1.1. Objectives 1](#_Toc35424791)

[1.2. Areas in scope 1](#_Toc35424792)

[1.3. Areas out of scope 4](#_Toc35424793)

[2. Project approach, timeline, and deliverable acceptance 5](#_Toc35424794)

[2.1. Approach 5](#_Toc35424795)

[2.2. Timeline 9](#_Toc35424796)

[2.3. Deliverable acceptance process 9](#_Toc35424797)

[2.4. Project governance 10](#_Toc35424798)

[2.5. Project completion 11](#_Toc35424799)

[3. Project organization 12](#_Toc35424800)

[3.1. Project roles and responsibilities 12](#_Toc35424801)

[4. Customer responsibilities and project assumptions 13](#_Toc35424802)

[4.1. Customer responsibilities 13](#_Toc35424803)

[4.2. Project assumptions 14](#_Toc35424804)

This Statement of Work (SOW) and any exhibits, appendices, schedules, and attachments to it are made pursuant to Work Order [insert Work Order number] and describes the work to be performed (Services) by Microsoft (“us,” “we”) for (“Customer,” “you,” “your”) relating to Security Modernization (project).

This SOW and the associated Work Order expire 30 days after their publication date, unless signed by both parties or formally extended in writing by Microsoft.

Introduction

# Project objectives and scope

## Objectives

The objective of this project is to modernize ’s security infrastructure to increase its network’s resilience to a cyber intrusion. The project will focus on delivering capabilities that help secure ’s on-premises environment through the implementation of Microsoft-recommended security controls in order to secure Azure Active Directory (Azure AD) and Active Directory Domain Services (AD DS) privileged accounts and administration operations.

The project consists of the following workstreams.

| Workstream | Capabilities | Description |
| --- | --- | --- |
| **Threat protection** | Identity security | Implement and configure Advanced Threat Analytics (ATA) to detect credential theft and anomalous behaviors in an AD DS environment based on known attack patterns and behavioral analytics. |

## Areas in scope

### General project scope

Microsoft will provide Services in support of the following scope.

* + - 1. Identity security

| Area | Description | Assumptions |
| --- | --- | --- |
| Advanced Threat Analytics (ATA) | * Implement ATA in [2] Active Directory Domain Services (AD DS) Forests:   + Enter the names of the In-Scope Forests * Assist with Customer-led remediation activities in preparation for the ATA implementation. * Help the Customer deploy up to [16] ATA Gateways or ATA Lightweight Gateways. * Configure syslog integration so that ATA forwards notifications to a syslog server. * Help the Customer tune the solution to address false-positive detections.   All Microsoft activities and assistance noted in this section are time-boxed to [80] hours. |  |

### Software products and technologies

The products and technology that are listed in the following table are required for project implementation. The Customer is responsible for obtaining all identified licenses and products.

**Important:** please consult with the Microsoft project manager to determine when the required software products and technologies need to be available, according to the project plan and key milestones.

| Scope area | Product and technology item |
| --- | --- |
| Advanced Threat Analytics | * Advanced Threat Analytics 1.9 or later * Windows Server 2012 R2 or later (Required for each ATA Center and standard ATA Gateway deployed as part of this engagement.) * Secure Sockets Layer (SSL) certificate for ATA Center service communication, server authentication (This is optional but a recommended feature to secure communication to the ATA center web portal). |

### Environments

The following environments will be required to deliver the project.

**IMPORTANT:** Please verify that these environments are available upon commencement of the Assess phase of the project.

| Environment | Location | Responsibility | Required for scope area |
| --- | --- | --- | --- |
| Production | Customer facilities | Customer | All |

### Testing and defect remediation

#### Testing

The following testing is included in the scope of the project. If additional time is needed for Microsoft testing support, then it can be requested through the Change management process described in this SOW.

| Test type (environment) | Description | Applies to scope area | Responsibility | | |
| --- | --- | --- | --- | --- | --- |
| Has responsibility  for testing? | Provides data or test cases | Provides guidance and support |
| User acceptance testing (UAT) | The user functionality of key real-world scenarios will be tested. | All | Customer | Customer | Microsoft |

#### Defect remediation

If defects are identified during testing, the priority of the item will be jointly agreed upon by the Customer and Microsoft. Defect prioritization is defined in the following table.

| Priority | Description | Remediation in scope? |
| --- | --- | --- |
| P1 | **Blocking defect**  Development, testing, or production launch cannot proceed until this type of defect is corrected. A defect of this type blocks further progress in this area. The solution cannot ship and the project team cannot achieve the next milestone until such a defect is corrected. | Yes |
| P2 | **Significant defect** This type of defect must be fixed prior to moving to production. Such a defect, however, will not affect test plan implementation. | Yes |
| P3 | **Important defect** It is important to correct this type of defect. However, it is possible to move forward into production through the use of a workaround. | No; the problem will be logged. Remediation will be performed through an agreed-upon change request only. |
| P4 | **Enhancements and low priority defects** P4 defects consist of feature enhancement and cosmetic defects. These include design requests that vary from original concepts. | No; the problem will be logged. Remediation will be performed through an agreed-upon change request only. |

## Areas out of scope

Any area not explicitly included in the Areas in scope section is out of scope for Microsoft during this project. Areas out of scope for this project are listed in the following table.

| Area | Description | |
| --- | --- | --- |
| Data migration | Data migration activities are out of scope. |
| Hardware | Procurement or installation of hardware required for this project is out of scope. |
| Integration with third-party software | Integrating any aspect of the solution with third-party software, unless specifically stated as in scope is out of scope. |
| Organizational change management | Designing—or redesigning—the Customer’s functional organization is not included. |
| Process reengineering | Design of functional business components of the solution is out of scope. |
| Product bugs  and upgrades | Product upgrades, bugs, and design change requests for Microsoft products are out of scope. |
| Product licenses and subscriptions | Product licenses (Microsoft or non-Microsoft) and cloud service subscriptions are out of scope. |
| Source code review | The Customer will not provide Microsoft with access to non-Microsoft source code or source code information. For any non-Microsoft code, Microsoft Services will be limited to the analysis of binary data, such as a process dump or network monitor trace. |
| Support | Ongoing operational support of the solution is out of scope. |
| System integration | * System integration and interfaces is out of scope |
| Advances Threat Analytics | The following are out of scope:   * Procurement of required SSL certificates. * Configuration of port mirroring for environments not using the ATA Lightweight Gateway. * Any integration of SIEM events into ATA. * Note: ATA relies on analyzing multiple network protocols and events collected from the SIEM or through Windows Event Forwarding. Detections based on network protocols with encrypted traffic (for example, LDAPS and IPSEC) are not analyzed. Domain controllers that use encrypted traffic are out of scope for this project. |

# Project approach, timeline, and deliverable acceptance

## Approach

The project will be structured following the Microsoft Online Services Lifecycle (OSL) methodology across four distinct phases: Assess, Remediate, Enable, and Migrate. Each phase has distinct activities and deliverables that are described in the following sections.

This project does not include any Migrate phase activities.

If a deliverable requires formal review and acceptance (a process described in the Deliverable acceptance process section), this is indicated in the following sections.

Assess

Enable

Remediate

Initiation

### Engagement initiation

Before beginning the project, the following prerequisites must be completed.

| Category | Description | |
| --- | --- | --- |
| **Microsoft activities** The activities to be performed by Microsoft | * Conduct a preinitiation call in order to initiate team formation and communicate expectations. * Document the project launch prerequisites using input from this SOW, including any resources the customer needs to provision for successful solution delivery. * Track the status of launch prerequisites and adjust the Engagement initiation phase start date accordingly. * Conduct a detailed walk-through of the SOW with the Customer in order to agree on an initial project schedule and approach. * Ensure any resources required for delivery of the solution, and in particular those needed during the ‘Assess’ phase, are available and meet the specifications provided by Microsoft. |
| **Customer activities** The activities to be performed by the Customer | * Attend and participate in the preinitiation call. * Assign project initiation and launch prerequisites responsibilities to accountable Customer leadership and establish target completion dates. * Complete the project initiation and launch prerequisites. * Staff the project with the required Customer resources in the time frames that were agreed upon in the preinitiation call. |

### Assess

|  | | |
| --- | --- | --- |
| Category | Description | |
| **Microsoft activities** The activities to be performed by Microsoft | **General activities**   * Conduct design workshops for each solution component. The workshops include technical overviews, component architecture and design, information about the Customer environment, Customer requirements and design decisions, and identification of remediation activities needed for implementation. * Create a preparation checklist for each solution component, that details the tasks that must be completed for implementation. * Create a design and plan document for each solution component that details the design and implementation process. |
| **Customer activities** The activities to be performed by the Customer | * Identify project team members and key project stakeholders. * Organize rooms and equipment needed for meetings and workshops. * Participate in meetings and workshops, communicate configuration requirements, provide current environmental information and documentation, and make design decisions. * Review and approve deliverables as required. * Initiate change control procedures that promote timely approval of modifications to be made to the production environment. |

#### Deliverables

| Name | Description | Acceptance required? | Responsibility |
| --- | --- | --- | --- |
| Preparation checklist | A Microsoft Excel spreadsheet that documents the tasks that must be completed by the Customer and the resources that must be procured in order to complete in-scope work | Yes | Microsoft |
| Design and plan | A Microsoft Word document that captures decisions made during the design workshops, documents the design for the solution, and details the high-level plan for the completion of in-scope work | Yes | Microsoft |
| Test cases | A Excel spreadsheet that documents the test cases that will be implemented to validate that the implemented solution functions as designed | No | Microsoft |

### Remediate

|  | | |
| --- | --- | --- |
| Category | Description | |
| **Microsoft activities** The activities to be performed by Microsoft | **General activities**   * Provide general guidance and support during Customer-led completion of identified preparation tasks. * Update the preparation checklist for each solution component, as required. * Update the design and plan document for each solution component, as required. |
| **Customer activities** The activities to be performed by the Customer | * Perform remediation activities, resolving or mitigating the items identified in the preparation checklist deliverable. * Provide feedback to Microsoft related to the design and plan and preparation checklist. * Manage all user communication associated with implementation. |
| **Key assumptions** | * The Customer is responsible for all remediation activities and will perform them with Microsoft assistance. Microsoft is not responsible for any remediation activities. * The Customer will communicate the actions taken and the results of those actions to Microsoft for inclusion in the updated preparation checklist and design and plan. |

#### Deliverables

| Name | Description | Acceptance required? | Responsibility |
| --- | --- | --- | --- |
| Preparation checklist | A Microsoft Excel spreadsheet that documents the actions taken and the results of those actions to Microsoft for inclusion in the updated preparation checklist and design and plan. | Yes | Microsoft |

### Enable

|  | | |
| --- | --- | --- |
| Category | Description | |
| **Microsoft activities** The activities to be performed by Microsoft | **General activities**   * Create test cases for each solution component that will be used to validate the solution functions as designed. * Implement solution components and configure them according to the design and plan documentation. * Perform system testing in order to validate the solution and remediate identified bugs and defects. * Finalize the design and plan document for each solution component. * Create a solution delivery summary document that summarizes the work completed for each solution component. |
| **Customer activities** The activities to be performed by the Customer | * Provision all hardware, software, subscriptions accounts, and other prerequisites required for implementation of the solution. * Manage organizational change and release management activities required for implementation. * Assist Microsoft, as necessary, during implementation tasks. * Perform testing and defect remediation activities as required. * Take ownership of the solution for ongoing management and support. * Review and accept all final work products and deliverables for the project. * Participate in knowledge and skills transfer workshops as required. |

#### Deliverables

| Name | Description | Acceptance required? | Responsibility |
| --- | --- | --- | --- |
| Delivery summary | A Word document that summarizes the work completed, provides any relevant maintenance guidance, and documents any recommended next steps | No | Microsoft |

## Timeline

During project planning, a detailed timeline will be developed. All dates and durations are relative to the project start date and are estimates only.

## Deliverable acceptance process

During the project, Microsoft will submit certain deliverables (listed in the Approach section as deliverables with “Acceptance required?” equal to “Yes”) for the Customer’s review and approval.

Within three business days of the date of submittal, the Customer is required to:

**Accept the deliverable** by signing, dating, and returning a service deliverable acceptance form, which can be sent by email, or by using (or partially using) the deliverable

Or

**Reject the deliverable** by notifying Microsoft in writing; the Customer must include a complete list of reasons for rejection.

**Review and acceptance** of the solution or custom source code is based on completion and acceptance of UAT as described in the Testing and defect remediation section.

A maximum of two (2) review cycles will be assigned to each documented Deliverable and feedback from these review cycles will be considered and incorporated into the document, where appropriate. Should acceptance require more than two (2) cycles, the Deliverable will be automatically escalated through the Escalation and resolution path process.

Problems that are outside the scope of this SOW, or feedback provided after a Deliverable has been accepted will be escalated through the Escalation and resolution path process.

Deliverables shall be deemed accepted unless the written rejection notification is received by Microsoft in the timeframe specified.

If a rejection notification is received, Microsoft will correct problems with a deliverable that are in scope for the project (and documented in this SOW), after which the deliverable is deemed accepted.

Problems that are outside the scope of this SOW, and feedback provided after a deliverable has been accepted will be addressed as a change request, managed as described in the Change management process section.

## Project governance

The governance structure and processes the team will adhere to for the project are described in the following sections:

### Project communication

The following will be used to communicate during the project:

* **Communication plan**: this document will describe the frequency, audience, and content of communication with the team and stakeholders. It will be developed by Microsoft and the Customer as part of project planning.
* **Status reports**: the Microsoft team will prepare and issue regular status reports to project stakeholders per the frequency defined in the communication plan.
* **Status meetings**: the Microsoft team will schedule regular status meetings to review the overall project status, the acceptance of deliverables, and review open problems and risks.

### Risk and issue management

The following general procedure will be used to manage active project issues and risks during the project:

* **Identify**: identify and document project issues (current problems) and risks (potential problems that could affect the project).
* **Analyze and prioritize**: assess the potential impact and determine the highest priority risks and problems that will be actively managed.
* **Plan and schedule**: determine the strategy for managing priority risks and issues, and identify a resource who can take responsibility for mitigation and remediation.
* **Track and report**: monitor and report the status of risks and problems.
* **Escalate**: escalate to project sponsors the high impact problems and risks that the team is unable to resolve.
* **Control**: review the effectiveness of risk and issue management actions.

Active issues and risks will be regularly monitored during the project.

### Change management process

During the project, either party is able to request modifications to the Services described in this SOW. These changes only take effect when the proposed change is agreed upon by both parties. The change management process steps are:

* **The change is documented**: all change requests will be documented by Microsoft in a Microsoft change request form and submitted to the Customer. The change request form includes:
  + A description of the change.
  + The estimated effect of implementing the change.
* **The change is submitted**: the change request form will be provided to the Customer.
* **The change is accepted or rejected**: the Customer has three business days to confirm the following to Microsoft:
  + Acceptance—the Customer must sign and return change request form.
  + Rejection—if the Customer does not want to proceed with the change or does not provide an approval within three business days, no changes will be performed.

### Executive steering committee

The executive steering committee provides overall senior management oversight and strategic direction for the project. The executive steering committee for the project will meet per the frequency defined in the communication plan and will include the roles listed in the following table. The responsibilities for the committee include:

* Making decisions about project strategic direction.
* Serving as a final arbiter of project issues.
* Approving significant change requests.

| Role | Organization | |
| --- | --- | --- |
| Project sponsor | Customer |
| Delivery manager | Microsoft |

### Escalation path

The Microsoft project manager will work closely with the Customer project manager, sponsor, and other designees to manage project issues, risks, and change requests as described previously. The Customer will provide reasonable access to the sponsor or sponsors in order to expedite resolution. The standard escalation path for review, approval, or dispute resolution is as follows:

* Project team member (Microsoft or the Customer)
* Project manager (Microsoft and the Customer)
* Microsoft delivery manager
* Microsoft and the Customer project sponsor
* Executive steering committee

## Project completion

Microsoft will provide Services defined in this SOW to the extent of the fees available and the term specified in the Work Order. If additional Services are required, the Change management process will be followed and the contract modified. The project will be considered complete when at least one of the following conditions has been met:

* All fees available have been utilized for Services delivered and expenses incurred.
* The term of the project has expired.
* All Microsoft activities and in-scope items have been completed.
* The Work Order has been terminated.

# Project organization

## Project roles and responsibilities

The key project roles and the responsibilities are as follows.

#### Customer

| Role | Responsibilities |
| --- | --- |
| Project sponsor | * Advocate for the project and necessary change within the organization. * Make key project decisions. * Serve as a point of escalation in order to support clearing project roadblocks. |
| Project manager | * Serve as the primary point of contact for the Microsoft team. * Manage the overall project. * Deliver the project on schedule. * Take responsibility for Customer resource allocation, risk management, and project priorities. * Communicate with executive stakeholders. |
| Lead architect | * Full time throughout project * Serve as primary technical point of contact. * Take ownership of technical architecture and deliverables. * Attend workshops and meetings as required and assist with decision making. |
| SMEs | * Be available for, and responsive to, technical, operational, or process questions as required. * Provide technical representation for the Customer’s environment. * Attend workshops and meetings as required and assist with decision making. * Assist with technical implementation of the solution into the Customer’s environment. * Subject matter expertise is required across the following areas (amongst others): * Security Architecture * Windows 10 and its security features * Active Directory and networking technologies (e.g. DNS, DHCP, etc.) * Azure and Azure Active Directory * Microsoft Threat Protection technologies |
| Test lead | * Be available for, and responsive to, technical, operational, or process questions as required. * Take responsibility for test plans and guides and coordinating the acceptance testing of resources. |

#### Microsoft

| Role | Responsibilities |
| --- | --- |
| Delivery manager | * Manage and coordinate the overall Microsoft project. * Serve as a single point of contact for escalations, billing problems, personnel matters, and contract extensions. |
| Microsoft project manager | * Manage and coordinate Microsoft project delivery. * Take responsibility for problem and risk management, change management, project priorities, status communications, and status meetings. * Coordinate Microsoft and Microsoft subcontractor resources but not Customer resources. |
| Microsoft lead architect | * Design the overall solution. * Provide guidance based on Microsoft-recommended practices. * Provide technical delivery oversight for the overall solution. * Review the quality of the deliverables. * Assist with risk management. |
| Microsoft consultants | * Provide technical oversight. * Verify whether Microsoft-recommended practices are being followed. * Take responsibility for implementation of solution components. * Take responsibility for documentation deliverables. |

# Customer responsibilities and project assumptions

## Customer responsibilities

In addition to Customer activities defined in the Approach section, the Customer is also required to:

* Provide information:
  + This includes accurate, timely (within three business days or as mutually agreed upon), and complete information.
* Provide access to people and resources.
  + This includes access to knowledgeable Customer personnel, including business user representatives, and access to funding if additional budget is needed to deliver project scope.
  + This includes the identification of key personnel (stakeholders, decision makers, architects, and subject matter specialists) to participate in the workshops, design sessions, and testing activities described in the Approach section.
  + This includes allocating enough qualified staff to run the workstreams in parallel.
* Provide access to systems.
  + This includes access to all necessary Customer work locations, networks, systems, and applications (remote and onsite).
  + The Customer is responsible for configuring and controlling all Azure subscriptions and consumption.
* Provide a work environment.
  + This consists of suitable work spaces, including desks, chairs, and Internet access.
* Manage non-Microsoft resources.
  + The Customer will assume responsibility for the management of all Customer personnel and vendors who are not managed by Microsoft.
* Manage external dependencies.
  + The Customer will facilitate any interactions with related projects or programs in order to manage external project dependencies.

## Project assumptions

The project scope, Services, fees, timeline, and our detailed solution are based on the information provided by the Customer to date. During the project, the information and assumptions in this SOW will be validated, and if a material difference is present, this could result in Microsoft initiating a change request to cover additional work or extend the project duration. In addition, the following assumptions have been made:

* Work day:
  + The standard work day for the Microsoft project team is between 8 AM and 5 PM, Monday through Friday.
  + When travel to a Customer location is required, the arrival time, especially on Mondays, might vary depending on the travel time. This also applies to departure time on Fridays.
* Standard holidays:
  + Observance of consultants’ country-of-residence holidays is assumed and has been factored into the project timeline.
* Remote working:
  + The Microsoft project team may perform Services remotely.
  + If the Microsoft project team is required to be present at the Customer location on a weekly basis, resources will typically be on site for three nights and four days, arriving on a Mondays and leaving on a Thursday.
* Language:
  + All project communications and documentation will be in English. Local language support and translations will be provided by the Customer.
* Staffing:
  + If necessary, Microsoft will make staffing changes. These can include, but are not limited to, the number of resources, individuals, and project roles.
  + Microsoft resources will be mobilized up to four weeks from the date of the Work Order signature.
  + If work is interrupted, the activities may be resumed once requested and agreed to by Microsoft. In this case Microsoft may require up to six weeks to mobilize the resources and have the complete project team in place. In this situation, Microsoft cannot guarantee that the team members will be the same team members who worked previously in the project.
* Informal knowledge transfer:
  + Customer staff members who work alongside Microsoft staff will be provided with information knowledge transfer throughout the project. No formal training materials will be developed or delivered as part of this informal knowledge transfer.